Journal of Discrete Algorithms 16 (2012) 249–257

Contents lists available at SciVerse ScienceDirect

Journal of Discrete Algorithms

www.elsevier.com/locate/jda

Quasi-cyclic codes over $\mathbb{F}_{13}$ and enumeration of defining polynomials

Vadlamudi Ch. Venkaiah [a,1], T. Aaron Gulliver [b,*]

[a] C.R. Rao Advanced Institute of Mathematics, Statistics, and Computer Science, University of Hyderabad Campus, Gachibowli, Hyderabad 500 046, India
[b] Department of Electrical and Computer Engineering, University of Victoria, Victoria, BC, Canada, V8W 3P6

ARTICLE INFO

Article history:
Available online 11 April 2012

Keywords:
Necklaces
Circulant matrices
Linear block codes
Finite fields

ABSTRACT

Let $d_q(n,k)$ be the maximum possible minimum Hamming distance of a linear $[n,k]$ code over $\mathbb{F}_q$. Tables of best known linear codes exist for small fields. In this paper, linear codes over $\mathbb{F}_{13}$ are constructed for k up to 6. The codes constructed are from the class of quasi-cyclic codes. The number of $m \times m$ circulant matrices over $\mathbb{F}_q$ is enumerated. In addition, the minimum distance of the extended quadratic residue code of length 44 is determined.

1. Introduction

Let $\mathbb{F}_q$ denote the finite field of q elements, and let $V(n,q)$ denote the vector space of all ordered n-tuples over $\mathbb{F}_q$. A linear $[n,k]$ code C of length n and dimension k over $\mathbb{F}_q$ is a k-dimensional subspace of $V(n,q)$. The elements of C are called codewords. The (Hamming) weight of a codeword is the number of nonzero coordinates. The minimum weight of C is the smallest weight among all nonzero codewords of C. The minimum weight of a linear code equals the minimum distance between codewords. An $[n,k,d]$ code is an $[n,k]$ code with minimum weight d. Let A_i be the number of codewords of weight i in C. Then the numbers $A_0, A_1, \ldots, A_n$ are called the weight distribution of C.

A central problem in coding theory is that of optimizing one of the parameters n, k and d for given values of the other two. One can find $d_q(n,k)$, the largest value of d for which there exists an $[n,k,d]$ code over $\mathbb{F}_q$, or $n_q(k,d)$, the smallest value of n for which there exists an $[n,k,d]$ code over $\mathbb{F}_q$. A code which achieves either of these values is called *optimal*. Tables of best known linear codes exist for all fields up to $q = 9$ [7]. In this paper, linear codes over $\mathbb{F}_{13}$ are constructed for k up to 6.

The Griesmer bound is a well-known lower bound on $n_q(k,d)$

$$n_q(k,d) \geqslant g_q(k,d) = \sum_{j=0}^{k-1} \left\lceil \frac{d}{q^j} \right\rceil, \tag{1}$$

where $\lceil x \rceil$ denotes the smallest integer $\geqslant x$. For $k \leqslant 2$, the Griesmer bound is met for all q and d. The Singleton bound [13] is a lower bound on $n_q(k,d)$ and is given by

$$n_q(k,d) \geqslant d + k - 1. \tag{2}$$

Codes that meet this bound are called maximum distance separable (MDS). MDS codes exist for all values of $n \leqslant q+1$. Thus for $q = 13$, MDS codes exist for all lengths 14 or less. Note that all MDS codes are optimal.

* Corresponding author.
E-mail addresses: venkaiah@hotmail.com (V.Ch. Venkaiah), agullive@ece.uvic.ca (T.A. Gulliver).

[1] This research was supported by the Department of Science and Technology, Govt. of India, New Delhi, under Project No.SR/S4/MS:516/07.

1570-8667/$ – see front matter
http://dx.doi.org/10.1016/j.jda.2012.04.006

For larger lengths and dimensions, far less is known about codes over $\mathbb{F}_{13}$. MDS self-dual codes ($k = n/2$), of lengths 2, 4, 6, 8, 10 and 14 are given in [1], as well as self-dual $[12, 6, 6]$, $[16, 8, 8]$, $[20, 10, 10]$, $[22, 11, 10]$ and $[24, 12, 10]$ codes. de Boer earlier discovered a self-dual $[18, 9, 9]$ code, and $[23, 3, 20]$ and $[23, 17, 6]$ codes [4]. The $[18, 9, 9]$, $[24, 12, 10]$ and $[30, 15, 12]$ extended quadratic residue (QR) codes are given in [14]. Using Magma [2], it was determined that the next extended QR code over $\mathbb{F}_{13}$ has parameters $[44, 22, 16]$. In this paper, codes with dimensions $k = 3$–6 are constructed. These codes establish lower bounds on the minimum distance. Many of these meet the Singleton and/or Griesmer bounds, and so are optimal.

A *punctured code* of C is a code obtained by deleting a coordinate from every codeword of C. A *shortened code* of C is a code obtained by taking only those codewords of C having a zero in a given coordinate position and then deleting that coordinate. The following bounds can be established based on these constructions

$$d_q(n+1,k) \leqslant d_q(n,k) + 1,$$

and

$$d_q(n+1,k+1) \leqslant d_q(n,k).$$

Using the codes given in this paper, they provide many additional lower bounds.

The next section presents the class of quasi-cyclic codes. Enumeration of the defining polynomials used to construct these codes is investigated in Section 3. The construction algorithm and results are given in Section 4.

2. Quasi-cyclic codes

A code C is said to be quasi-cyclic (QC) if a cyclic shift[2] of any codeword by p positions is also a codeword in C. The length of a QC code is then $n = mp$ [8]. A cyclic code is a QC code with $p = 1$. With a suitable permutation of coordinates, many QC codes can be characterized in terms of $m \times m$ circulant matrices. In this case, a QC code can be transformed into an equivalent code with generator matrix

$$G = [R_0\ R_1\ R_2\ \ldots\ R_{p-1}], \tag{3}$$

where R_i, $i = 0, 1, \ldots, p-1$, is a circulant matrix of the form

$$R_i = \begin{bmatrix} r_{0,i} & r_{1,i} & r_{2,i} & \cdots & r_{m-1,i} \\ r_{m-1,i} & r_{0,i} & r_{1,i} & \cdots & r_{m-2,i} \\ r_{m-2,i} & r_{m-1,i} & r_{0,i} & \cdots & r_{m-3,i} \\ \vdots & \vdots & \vdots & & \vdots \\ r_{1,i} & r_{2,i} & r_{3,i} & \cdots & r_{0,i} \end{bmatrix}. \tag{4}$$

The algebra of $m \times m$ circulant matrices over $\mathbb{F}_q$ is isomorphic to the algebra of polynomials in the ring $\mathbb{F}_q[x]/(x^m - 1)$ if R_i is mapped onto the polynomial $r_i(x) = r_{0,i} + r_{1,i}x + r_{2,i}x^2 + \cdots + r_{m-1,i}x^{m-1}$, formed from the entries in the first row of R_i [13]. The $r_i(x)$ associated with a QC code are called the *defining polynomials* [8]. The set $\{r_0(x), r_1(x), \ldots, r_{p-1}(x)\}$ defines an $[mp, m]$ QC code with $k = m$.

3. Necklaces and defining polynomials

The construction of QC codes requires a representative set of defining polynomials. These are the equivalence class representatives of a partition of the set of polynomials of degree less than m. Two polynomials $r_j(x)$ and $r_i(x)$ are said to be *equivalent* if they belong to the same class, i.e.

$$r_j(x) = \gamma x^l r_i(x) \mod\left(x^m - 1\right),$$

for some integer $l \geqslant 0$ and scalar $\gamma \in \mathbb{F}_q \setminus \{0\}$.

The defining polynomials are similar to necklaces, which are the equivalence classes under cyclic rotation. The number of length m necklaces over $\mathbb{F}_q$ is [16, p. 75]

$$a(m,q) = \frac{1}{m}\sum_{d|m} \phi(d) q^{m/d}.$$

For the defining polynomials, multiplication by a nonzero element of $\mathbb{F}_q$ does not change the weight and hence does not change the equivalence class. Thus, the number of defining polynomials differs from the number of necklaces. Enumeration of the defining polynomials is considered below.

[2] A cyclic shift of an m-tuple $(x_0, x_1, \ldots, x_{m-1})$ is the m-tuple $(x_{m-1}, x_0, \ldots, x_{m-2})$.

Let t be an element of $\mathbb{F}_q \setminus \{0\}$ and let g be the permutation $(1, 2, \ldots, m)$. That is, g maps i to $i+1$ and m to 1. Therefore, g^i, $1 \leqslant i \leqslant m$, is also a permutation and has order $\frac{m}{\gcd(m,i)}$ in the symmetric group of degree m. The disjoint cycle decomposition of g^i consists of $\gcd(m, i)$ cycles, and the length of each cycle is equal to the order of g^i, which is $\frac{m}{\gcd(m,i)}$.

Definition 1. An ordered m-tuple (or word of length m), $x = (x_1, x_2, \ldots, x_m)$, is said to be fixed by tg^i, $t \in \mathbb{F}_q \setminus \{0\}$, $1 \leqslant i \leqslant m$, if the m-tuple x remains unaltered after the following two operations are carried out in any order.

(i) Permutation of x according to g^i, and
(ii) multiplication by t followed by modulo q reduction of each component of the m-tuple

Lemma 1. *A nonzero word of length m over $\mathbb{F}_q$ is fixed by tg^i, $t \in \mathbb{F}_q \setminus \{0\}$, $1 \leqslant i \leqslant m$, if and only if the order of t, $\mathrm{ord}_q(t)$, in the multiplicative group of $\mathbb{F}_q$ divides the order of g^i in the symmetric group of degree m.*

Proof. Fix i such that $1 \leqslant i \leqslant m$ and let $x = (x_1, x_2, \ldots, x_m)$ be a nonzero word of length m. Let $r = \gcd(m, i)$ and $\ell = \frac{m}{r}$. Then the permutation g^i is a product of r disjoint cycles and each cycle is of length ℓ. Let $\alpha = (a_1, a_2, \ldots, a_\ell)$ be an arbitrary cycle of these r cycles. The action of g^i on x causes the action of α on the ℓ components, which sends the a_{i-1}th component of x to the a_ith position for $2 \leqslant i \leqslant \ell$, and the a_ℓth component of x to the a_1th position. Similarly, the action of tg^i, $t \in \mathbb{F}_q \setminus \{0\}$, on x causes the a_{i-1}th component of x to go to the a_ith position, to become $(tx_{a_{i-1}}) \bmod q$. Thus, the ℓ components $(x_{a_1}, x_{a_2}, \ldots, x_{a_\ell})$ of the word x are fixed by tg^i if and only if

$$\begin{aligned}
x_{a_1} &= (tx_{a_\ell}) \mod q \\
x_{a_2} &= (tx_{a_1}) \mod q = \left(t^2 x_{a_\ell}\right) \mod q \\
x_{a_3} &= (tx_{a_2}) \mod q = \left(t^3 x_{a_\ell}\right) \mod q \\
&\vdots \\
x_{a_\ell} &= (tx_{a_{\ell-1}}) \bmod q = \left(t^\ell x_{a_\ell}\right) \bmod q
\end{aligned} \tag{5}$$

Since x is a nonzero word, this is true if and only if $t^\ell \equiv 1 \bmod q$. Therefore the order of t must be a divisor of ℓ. Since α is arbitrary, this holds for all the cycles in the cycle decomposition of g^i. The result then follows because ℓ is the order of the permutation g^i. □

Theorem 2. *The number of words of length m over $\mathbb{F}_q$ fixed by tg^i, $t \in \mathbb{F}_q \setminus \{0\}$, $1 \leqslant i \leqslant m$, is equal to the number of words fixed by the corresponding permutation g^i if the order of t, $\mathrm{ord}_q(t)$, in the multiplicative group of $\mathbb{F}_q$ divides the order of g^i in the symmetric group of degree m. Otherwise, the number of words fixed by tg^i is 1, which is the all zero word.*

Proof. From Lemma 1, we have that a nonzero word is fixed if and only if the order of t divides the order of g^i. Also, since x_{a_ℓ} can take q values, there are q ways that (5) can be satisfied. Since there are $\gcd(m, i)$ cycles, it follows that the number of words fixed by tg^i is equal to $q^{\gcd(m,i)}$. This is also the number fixed by g^i. The all zero word is fixed irrespective of the orders of t and g^i. Hence the theorem results. □

Definition 2. Two circulant matrices over $\mathbb{F}_q$ are equivalent if the first row of one of the matrices is equal to a nonzero constant multiple of one of the rows of the other.

Clearly, this is an equivalence relation on the set of circulant matrices. The following theorem determines the corresponding number of equivalence classes.

Theorem 3. *The number of equivalence classes of $m \times m$ circulant matrices over $\mathbb{F}_q$ is*

$$c(m, q) = \frac{1}{(q-1)m} \sum_{d|m} \Bigg[\sum_{\substack{i|d \\ i|q-1}} \left(\phi(i)\phi(d)q^{m/d}\right) + \phi(d)\left(q - 1 - \sum_{\substack{i|d \\ i|q-1}} \phi(i)\right)\Bigg]. \tag{6}$$

Proof. Note that there are $(q-1)m$ permutations given by tg^j, $t \in \mathbb{F}_q \setminus \{0\}$, $1 \leqslant j \leqslant m$. Thus, by Burnside's Lemma [5], the number of orbits of words of length m over an alphabet of size q is equal to the average number of words fixed by each tg^j, $t \in \mathbb{F}_q \setminus \{0\}$, $1 \leqslant j \leqslant m$. Therefore we have

$$c(m,q) = \frac{1}{(q-1)m} \sum_{\substack{j=1 \\ t\in\mathbb{F}_q\setminus\{0\}}}^{m} \left|\mathrm{Fix}\left(tg^j\right)\right|,$$

where $|\mathrm{Fix}(tg^j)|$ denotes the number of words fixed by tg^j.

From Theorem 2, the number of words fixed by tg^j, $t \in \mathbb{F}_q \setminus \{0\}$, is either equal to the number of elements fixed by g^j, $1 \leqslant j \leqslant m$, if the order of t in the multiplicative group of $\mathbb{F}_q$ divides the order of g^j in the symmetric group of degree m, or else it is equal to one. It must then be that

$$\begin{aligned}
c(m,q) &= \frac{1}{(q-1)m} \sum_{j=1}^{m} \left\{ \sum_{\substack{t\in\mathbb{F}_q\setminus\{0\} \\ ord_q(t)\mid ord(g^j)}} \left|\mathrm{Fix}\left(tg^j\right)\right| + \sum_{\substack{t\in\mathbb{F}_q\setminus\{0\} \\ ord_q(t)\nmid ord(g^j)}} 1 \right\} \\
&= \frac{1}{(q-1)m} \sum_{j=1}^{m} \left\{ \sum_{\substack{t\in\mathbb{F}_q\setminus\{0\} \\ ord_q(t)\mid ord(g^j)}} \left|\mathrm{Fix}\left(tg^j\right)\right| + \left((q-1) - \sum_{\substack{t\in\mathbb{F}_q\setminus\{0\} \\ ord_q(t)\mid ord(g^j)}} 1 \right) \right\} \\
&\quad (\because \text{ there are } q-1 \text{ nonzero elements in } \mathbb{F}_q) \\
&= \frac{1}{(q-1)m} \sum_{j=1}^{m} \left\{ \sum_{\substack{t\in\mathbb{F}_q\setminus\{0\} \\ ord_q(t)\mid ord(g^j)}} \left|\mathrm{Fix}\left(g^j\right)\right| + \left((q-1) - \sum_{\substack{t\in\mathbb{F}_q\setminus\{0\} \\ ord_q(t)\mid ord(g^j)}} 1 \right) \right\} \\
&= \frac{1}{(q-1)m} \sum_{j=1}^{m} \left\{ \sum_{\substack{t\in\mathbb{F}_q\setminus\{0\} \\ ord_q(t)\mid ord(g^j)}} \left[\left|\mathrm{Fix}\, g^j\right| - 1\right] + (q-1) \right\}.
\end{aligned}$$

The number of words fixed by g^j, $1 \leqslant j \leqslant m$, is completely determined by the number of cycles in the cycle decomposition of g [15]. Thus if g has c cycles, then it fixes q^c words. Since the number of cycles in g^j, $1 \leqslant j \leqslant m$, is $\frac{m}{ord(g^j)}$ and the order of g^j in the symmetric group of degree m is $\frac{m}{\gcd(m,j)}$, it follows that g^j has $\gcd(m,j)$ cycles. Therefore we have

$$c(m,q) = \frac{1}{(q-1)m} \sum_{j=1}^{m} \left\{ \sum_{\substack{t\in\mathbb{F}_q\setminus\{0\} \\ ord_q(t)\mid ord(g^j)}} \left[q^{\gcd(m,j)} - 1\right] + (q-1) \right\}. \tag{7}$$

Since there are $\phi(i)$ elements of order i in the multiplicative group of $\mathbb{F}_q \setminus \{0\}$, (7) can be written as

$$c(m,q) = \frac{1}{(q-1)m} \sum_{j=1}^{m} \left\{ \sum_{\substack{i\mid(q-1) \\ i\mid ord(g^j)}} \phi(i)\left[q^{\gcd(m,j)} - 1\right] + (q-1) \right\}.$$

As there are $\phi(d)$ elements of order d in the symmetric group of degree m, and the order of an element in g^j is $\frac{m}{\gcd(m,j)}$, we have

$$\begin{aligned}
c(m,q) &= \frac{1}{(q-1)m} \sum_{d\mid m} \phi(d) \left\{ \sum_{\substack{i\mid(q-1) \\ i\mid d}} \phi(i)\left[q^{m/d} - 1\right] + (q-1) \right\} \\
&= \frac{1}{(q-1)m} \sum_{d\mid m} \left\{ \sum_{\substack{i\mid(q-1) \\ i\mid d}} \phi(i)\phi(d) q^{m/d} + \phi(d)\left((q-1) - \sum_{\substack{i\mid(q-1) \\ i\mid d}} \phi(i) \right) \right\}. \qquad \square
\end{aligned}$$

Corollary 4. *The number of nonzero defining polynomials for $m \times m$ circulant matrices over $\mathbb{F}_q$ is*

$$b(m,q) = \frac{1}{(q-1)m} \sum_{d\mid m} \phi(d)\left(q^{m/d} - 1\right) \gcd(d, q-1).$$

Proof. From Theorem 3, we have

$$
\begin{aligned}
c(m,q) &= \frac{1}{(q-1)m}\sum_{d|m}\Bigg[\sum_{\substack{i|d\\ i|q-1}}\phi(i)\phi(d)q^{m/d}+\phi(d)\Bigg(q-1-\sum_{\substack{i|d\\ i|q-1}}\phi(i)\Bigg)\Bigg]\\
&= \frac{1}{(q-1)m}\sum_{d|m}\big[\phi(d)\gcd(d,q-1)q^{m/d}+\phi(d)\big(q-1-\gcd(d,q-1)\big)\big]\\
&\quad\Bigg(\because \sum_{\substack{i|d\\ i|(q-1)}}\phi(i)=\gcd\big(d,(q-1)\big)\Bigg)\\
&= \frac{1}{(q-1)m}\sum_{d|m}\phi(d)\big[\gcd(d,q-1)\big(q^{m/d}-1\big)+q-1\big]\\
&= \frac{1}{(q-1)m}\sum_{d|m}\phi(d)\gcd(d,q-1)\big(q^{m/d}-1\big)+\frac{1}{(q-1)m}\sum_{d|m}\phi(d)(q-1)\\
&= \frac{1}{(q-1)m}\sum_{d|m}\phi(d)\gcd(d,q-1)\big(q^{m/d}-1\big)+1\quad\Bigg(\because\sum_{d|m}\phi(d)=m\Bigg).
\end{aligned}
$$

Since the zero polynomial is not considered, the result follows. □

Thus for $q=2$, $a(m,q)=b(m,q)$, and for $q=3$, $a(m,q)=b(m,q)/2$ for m odd. The result for $q=3$ was presented in a different form in [9].

From Corollary 4, the number of nonzero defining polynomials, $b(m,q)=c(m,q)-1$, for $m=2$ to 6 and $q=\mathbb{F}_{13}$ $N(m)=b(m,q)$ is given below.

m	$N(m)$
2	8
3	63
4	604
5	6189
6	67116

4. The construction algorithm and results

Imposing a structure on the codes being considered results in a search space that is smaller than for the general code design problem. The more restrictions on the structure, the smaller the search, but this results in a tradeoff, since good codes may be missed if too much structure is imposed on the code. The QC codes presented here were constructed using a stochastic optimization algorithm, tabu search, similar to that in [3,10] and [11]. By restricting the search for good codes to the class of QC codes, and using a stochastic heuristic, codes with high minimum distance can be found with a reasonable amount of computational effort. Based on the results obtained here, this approach provides a good tradeoff.

It is not necessary to check the weight of every codeword in a QC code in order to determine the minimum distance d. Only a subset of the codewords need be considered since the Hamming weight of $i(x)b_s(x) \bmod(x^m-1)$ is equal to the weight of $i(x)\gamma x^l b_s(x) \bmod(x^m-1)$ for all $l \geqslant 0$ and $\gamma \in \mathbb{F}_q \setminus \{0\}$. Note that this argument also applies to the set of defining polynomials. For example, with $q=13$ and $m=3$, from the above table $N(m)=63$.

To simplify the process of searching for good codes, the weights of the subset of codewords can be stored in an array, and a matrix D formed from the arrays for the defining polynomials to be considered

$$
D=\begin{array}{c|cccccc}
 & b_1(x) & b_2(x) & \cdots & b_s(x) & \cdots & b_y(x)\\ \hline
i_1(x) & w_{11} & w_{12} & \cdots & w_{1s} & \cdots & w_{1y}\\
i_2(x) & w_{21} & w_{22} & \cdots & w_{2s} & \cdots & w_{2y}\\
\vdots & \vdots & \vdots & & \vdots & & \vdots\\
i_t(x) & w_{t1} & w_{t2} & \cdots & w_{ts} & \cdots & w_{ty}\\
\vdots & \vdots & \vdots & & \vdots & & \vdots\\
i_z(x) & w_{z1} & w_{z2} & \cdots & w_{zs} & \cdots & w_{zy},
\end{array}
$$

where $i_t(x)$ is the tth information polynomial, $b_s(x)$ is the sth defining polynomial, and w_{ts} is the Hamming weight of $i_t(x)b_s(x) \bmod(x^m-1)$. Since the $i_t(x)$ and $b_s(x)$ correspond to the same set of polynomials, D is a square ($y=z=N(m)$),

symmetric (by letting $i_t(x) = b_t(x)$ for all $1 \leqslant t \leqslant N(m)$), matrix. For example, if $q = 13$ and $m = 2$, the matrix is

$$D = \begin{array}{c|cccccccc} & 1 & x+1 & x+2 & x+3 & x+4 & x+5 & x+6 & x+12 \\ \hline 1 & 1 & 2 & 2 & 2 & 2 & 2 & 2 & 2 \\ x+1 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 0 \\ x+2 & 2 & 2 & 2 & 2 & 2 & 2 & 1 & 2 \\ x+3 & 2 & 2 & 2 & 2 & 1 & 2 & 2 & 2 \\ x+4 & 2 & 2 & 2 & 1 & 2 & 2 & 2 & 2 \\ x+5 & 2 & 2 & 2 & 2 & 2 & 1 & 2 & 2 \\ x+6 & 2 & 2 & 1 & 2 & 2 & 2 & 2 & 2 \\ x+12 & 2 & 0 & 2 & 2 & 2 & 2 & 2 & 2 \end{array}$$

The complete weight distribution for a QC code composed of any set of $b_s(x)$ can be constructed from D. The search for a good code consists of finding p columns of D with a large minimum row sum, since the weight of a minimum distance codeword must be contained in these sums.

Having decided on the values of m and p (and thus also $n = mp$), the entries of the integer matrix D can be calculated and the problem formulated as a combinatorial optimization problem. The goal is to find

$$\max_{S} \min_{1 \leqslant j \leqslant N} \sum_{s \in S} w_{j,s}, \tag{8}$$

where $S \subseteq \{1, 2, \ldots, N\}$ and $|S| = p$. In general, one can take a multiset S with p elements, but it was found in past studies that for the new codes obtained, no defining polynomial occurs more than once, so S is here required to be a set.

The optimization method used here is *tabu search* [6]. This method can produce good optimal or near-optimal solutions to intractable optimization problems with a reasonable amount of computational effort [12]. Tabu search is a local search algorithm, which means that starting from an initial solution, a series of solutions is obtained so that every new solution only differs slightly from the previous one. A potential new solution is called a *neighbor* of the old solution, and all neighbors of a given solution constitute the *neighborhood* of that solution. To evaluate the quality of solutions, a *cost function* is needed. Tabu search always proceeds to a best possible solution in the neighborhood of the current solution. To ensure that the search does not loop on a subset of moves or solutions, attributes of recent solutions are stored in a tabu list. New moves or solutions with attributes from this list are then not allowed for L moves.

Tabu search is applied here to the problem of finding QC codes, defined as a minimization problem, in the following way. First, the problem is not formulated as generally as in (8), as the desired minimum distance, d, of the code is fixed. A solution is any set $S \subseteq \{1, 2, \ldots, N\}$ of p columns of D, the neighborhood of a solution is the set of solutions obtained by replacing one column with a column that is not in the code, and the cost function is of the form

$$C = \sum_{j=1}^{N} \max\left(0, d - \sum_{s \in S} w_{j,s}\right).$$

A solution with cost 0 then corresponds to a code with minimum distance at least d. If such a solution is found, the search ends. Otherwise, the search is continued (and typically restarted occasionally), until a given time or iteration limit is reached. The tabu list is simply the indexes of the new columns.

The values of L used were small, in the range $p/10 \leqslant L \leqslant p/5$. If a code was not found within 100–2000 iterations, the search was restarted from a new random initial solution. As many as 10 000 restarts were performed for given values of m and p. The total number of iterations to find a code varied from hundreds to millions.

The best QC codes found are given in Tables 1 to 4. The defining polynomials are listed with the lowest degree coefficient on the left, i.e., 7321 corresponds to the polynomial $x^3 + 2x^2 + 3x + 7$, with leading zeroes left out for brevity. The digits 10, 11 and 12 are denoted by (10), (11) and (12), respectively. As an example, consider the [18, 3] code in Table 1 with $m = 3$ and $p = 6$ defining polynomials. These polynomials give the following generator matrix

$$G = \left[\begin{array}{c|c|c|c|c|c} 016 & 175 & 125 & 117 & 135 & 143 \\ 601 & 517 & 512 & 711 & 513 & 314 \\ 160 & 751 & 251 & 171 & 351 & 431 \end{array}\right]$$

with weight distribution

i	A_i
0	1
15	456
16	468
17	720
18	552

Table 1
Best QC codes over $\mathbb{F}_{13}$ with $p = 3$.

Code	d	$r_i(x)$
[6, 3]	4	1, 12(12)
[9, 3]	7	1, 15(11), 117
[12, 3]	10	1, 135, 112, 153
[15, 3]	12	11, 153, 12, 143, 11(10)
[18, 3]	15	16, 175, 125, 117, 135, 143
[21, 3]	18	115, 11(10), 146, 132, 16, 1, 176
[24, 3]	20	1, 174, 1(11), 112, 19(12), 138, 114, 12(12)
[27, 3]	23	112, 117, 12, 162, 17, 12(12), 13, 114, 19
[30, 3]	26	124, 176, 11(12), 156, 13, 129, 13(11), 14, 17, 132
[33, 3]	29	12, 1(10), 13(11), 18, 15, 12(12), 15(11), 132, 156, 126, 116
[36, 3]	32	129, 11(10), 11, 11(11), 19, 146, 12(12), 14(11), 11(12), 145, 13, 18
[39, 3]	34	1(11), 138, 12, 11, 14(11), 11(11), 16, 125, 112, 114, 113, 156, 15
[42, 3]	37	15, 12, 119, 158, 126, 156, 138, 11(12), 11, 176, 117, 1(11), 112, 13(10)
[45, 3]	40	18, 1(11), 163, 11, 134, 135, 126, 156, 174, 19(12), 17, 132, 125, 13, 162
[48, 3]	43	116, 1(10), 1(11), 114, 14(11), 142, 1(10)6, 12(12), 19(12), 163, 11(12), 12, 174, 146, 11, 1(12)
[51, 3]	45	113, 16, 11, 17, 142, 146, 18, 118, 132, 194, 1(12), 156, 15, 117, 176, 116, 115
[54, 3]	48	17, 11, 13(12), 132, 118, 19, 153, 185, 13(10), 14(11), 146, 162, 142, 11(11), 135, 175, 15, 11(10)
[57, 3]	51	1(11), 11(10), 175, 123, 12(12), 115, 156, 1, 163, 124, 13, 18, 11(12), 11(11), 146, 112, 19, 17(12), 132
[60, 3]	54	162, 11(12), 13, 118, 113, 115, 13(12), 117, 19, 18, 112, 12, 185, 138, 153, 123, 17, 156, 126, 132
[63, 3]	56	116, 143, 119, 185, 146, 15(11), 11, 134, 19(12), 117, 156, 115, 19, 135, 12(11), 15, 158, 125, 154, 113, 18
[66, 3]	59	118, 1, 11(11), 13(12), 135, 154, 17, 11, 13(11), 163, 12(10), 129, 112, 115, 15, 12(11), 19(12), 119, 132, 19, 18, 123
[69, 3]	62	18, 142, 19, 11(11), 194, 17, 14(11), 13(11), 118, 132, 11, 123, 125, 112, 113, 12(10), 156, 17(12), 16, 117, 129, 116, 1(11)
[72, 3]	65	1(12), 134, 1(11), 17(12), 119, 1, 11, 15(11), 163, 13(10), 124, 114, 142, 13, 128, 14(11), 154, 126, 11(12), 11(11), 156, 19, 117, 176

Table 2
Best QC codes over $\mathbb{F}_{13}$ with $p = 4$.

Code	d	$r_i(x)$
[8, 4]	5	1135, 1326
[12, 4]	9	104, 1197, 135
[16, 4]	12	17, 1(10)3, 14(11)8, 161(11)
[20, 4]	16	116, 1(11), 1186, 142, 134(10)
[24, 4]	19	1326, 11, 1745, 111(11), 186, 1165
[28, 4]	23	14, 13, 1159, 163(11), 1252, 112(12), 1294
[32, 4]	26	103, 1(10)3, 1182, 114, 1143, 1(10)(10), 1132, 1(11)(10)
[36, 4]	30	1155, 113, 139, 1117, 13(10)(11), 153(11), 125, 136, 122
[40, 4]	33	12, 1315, 1, 115(10), 141, 117(10), 1825, 112(12), 1(12)4, 1184
[44, 4]	37	14, 1118, 112(10), 11(11)(12), 113(10), 102, 1214, 12(10)4, 1(11), 13(10), 13(12)2
[48, 4]	40	102, 1115, 12, 1166, 12(10)4, 133, 18(11), 145(11), 12(10)5, 1197, 1825, 112(12)
[52, 4]	44	11, 1, 1125, 1546, 12(11)6, 1(12)5, 11(10)4, 1293, 1135, 1197, 17(10), 1458, 168
[56, 4]	48	103, 19, 1(11)6, 1112, 145(11), 17(10), 141, 13(10)6, 1376, 1385, 119(10), 11(10)9, 11(12)8, 1(10)7
[60, 4]	51	11, 135, 153, 1598, 169, 13(11)(12), 123, 1112, 12(12), 1416, 128(12), 1346, 1219, 118(10), 181
[64, 4]	55	135, 14(10)5, 151, 11(11)(10), 1418, 166, 13(10)5, 13(11)2, 1564, 16(10), 14(11)(12), 1193, 1153, 14, 1116, 111(10)
[68, 4]	58	1, 112, 14(10)2, 1592, 1265, 17(10), 151(11), 167(12), 193, 145(12), 1416, 117, 1115, 189, 1464, 14(12), 135
[72, 4]	62	13, 1623, 1243, 1462, 1475, 12, 172, 1128, 161(11), 164, 1535, 12(12), 1625, 1148, 1284, 134, 18(12), 1328
[76, 4]	66	171, 1284, 1376, 12(11)3, 113(12), 12(10), 1, 11(10)3, 161(12), 1154, 143, 1289, 12(10)(11), 119(11), 1(11)(12), 129(12), 187, 1278, 1318
[80, 4]	69	105, 11(10)(11), 1825, 1314, 1(12)(12), 102, 14(10)(11), 113, 11(12), 1423, 127(12), 124(10), 1148, 1243, 1215, 12(11)6, 1329, 127, 1(11), 1382
[84, 4]	73	196, 1376, 158, 167, 18(10)3, 1343, 129, 14(12), 1, 1498, 1187, 133, 143(10), 1237, 1(11)5, 1598, 1217, 1172, 125, 12(11)2, 1238
[88, 4]	76	11, 1245, 1, 1585, 113(12), 112(12), 1329, 1(12)(10), 1876, 197, 199, 1138, 121(11), 1(11)6, 17(11), 1354, 15(11)6, 1134, 17(10), 1684, 1319, 14(10)
[92, 4]	80	102, 1169, 149, 16(12), 1, 146, 1(12)(12), 1384, 1172, 1425, 1114, 1(10)1, 115, 1217, 192, 12(11)3, 147(12), 1193, 1456, 1454, 1756, 127(10), 11(12)6
[96, 4]	84	113, 1415, 1, 1254, 1(12)(12), 137(11), 13(11)3, 119(11), 187, 13, 11(11)9, 1194, 1623, 13(12)2, 1264, 11(10), 1516, 11(11)5, 145(11), 128(11), 1148, 106, 121, 129(10)

This code is optimal since it meets the Griesmer bound (1), and so establishes that $d_{13}(18, 3) = 15$.

For $m = 5$ and $p = 4$, the best code found has generator matrix

$$G = \left[\begin{array}{c|c|c|c} 00018 & 14(10)(12)4 & 01(12)8(11) & 12(11)3(12) \\ 80001 & 414(10)(12) & (11)01(12)8 & (12)12(11)3 \\ 18000 & (12)414(10) & 8(11)01(12) & 3(12)12(11) \\ 01800 & (10)(12)414 & (12)8(11)01 & (11)3(12)12 \\ 00180 & 4(10)(12)41 & 1(12)8(11)0 & 2(11)3(12)1 \end{array}\right]$$

Table 3
Best QC codes over $\mathbb{F}_{13}$ with $p = 5$.

Code	d	$r_i(x)$
[10, 5]	6	13(10), 10(10)(10)
[15, 5]	10	154, 14(10)56, 11(12)9(10)
[20, 5]	15	18, 14(10)(12)4, 1(12)8(11), 12(11)3(12)
[25, 5]	19	10(12), 1(12)(11)(12), 14168, 11893, 17(10)(12)3
[30, 5]	23	1561(11), 11659, 1163(12), 1(10)6(11), 126(10)(12), 1842
[35, 5]	27	10(10), 112(12)6, 16842, 11458, 11(10)(12), 1212(12), 11(10)92
[40, 5]	31	1, 13(12)1, 12434, 1157, 158(12)3, 133(10), 11(12)3(11), 111
[45, 5]	36	11(10), 19, 11453, 1156(12), 12(12)5, 11247, 16746, 1222, 1635(11)
[50, 5]	40	121(10)2, 14, 12619, 1(12)47, 12(12)2(12), 1454, 11586, 12835, 13792, 13(10)(12)
[55, 5]	45	138(12)8, 11, 1(10)3(10)6, 159, 172(11), 12348, 1673(11), 10(12)(12), 15684, 128(11)8, 1776
[60, 5]	49	13, 1589, 11284, 1333, 11(11), 153, 1456, 12(12)52, 13(12)6(11), 12(11)89, 1(11)1(12), 11724
[65, 5]	54	16(12), 1(10)94, 128(10)(11), 10(11)9, 1(11)11, 13(11)6, 11(12)49, 13138, 1152(11), 1351(10), 11139, 1124(10), 14(11)
[70, 5]	58	103, 14, 17(12)34, 12(11)(10)(12), 124(10)(11), 112, 1713, 11(11)89, 14182, 106(12), 11374, 11553, 1(10)17, 145(11)3
[75, 5]	62	1137, 11, 103, 1161(12), 1(10)9, 1987, 1(12)32, 1783, 11766, 142(11)3, 11618, 12(12)43, 141(12)2, 127(11)5, 1152(12)
[80, 5]	67	152, 102, 14(11)3(11), 15(10), 11(12)7(10), 1385, 11(11)38, 11229, 11295, 15385, 1334, 18(11)6, 1115(12), 12154, 1841, 11(11)8
[85, 5]	71	1944, 13, 1268(11), 1(11)92, 12(12)72, 119, 1131(10), 1841, 15(11)5, 129(10)6, 1497(12), 11(12)82, 15325, 11584, 14742, 14(10)(11)3, 1397(10)
[90, 5]	76	122, 1675(11), 1262(12), 12825, 113(11)5, 15(12)(11), 1(11)8, 1(10)4, 12(10)3(10), 1394(12), 119(12)9, 1172(12), 12723, 1552, 121, 12(12)8(11), 14(11)(10)(11), 19(12)
[95, 5]	80	14(10), 12978, 14, 11474, 11(11)7(11), 14(11)2(11), 1285, 127, 12132, 14646, 1955, 12(11)63, 134(10)2, 14934, 11(12)96, 1(12), 1627(12), 14163, 119(12)8
[100, 5]	84	135, 11(11)96, 15(10), 13494, 1241(11), 127(10)(12), 13(10)23, 11(10)2(11), 137(11), 13156, 13(10)28, 13(10)6(10), 1(10)95, 128(12)3, 12496, 1134(11), 159(11)8, 11917, 19(10)(10), 13(11)2(11)
[105, 5]	89	108, 11445, 14(11)2, 12328, 14(11)82, 11833, 135(11)4, 18(10)9(12), 11269, 114(12)5, 13172, 173(10), 144(12), 11(10)3, 142(12)4, 16975, 117(12)7, 113(11)8, 11(12)(11)3, 12(10)3(12), 11875
[110, 5]	93	106, 1121(11), 14(10)(11), 111, 161(12)6, 12694, 193, 14172, 11564, 1117(12), 13(10)4, 1(11)3(10), 115(10)8, 12349, 1131(12), 14374, 161(11)2, 1721, 11(12)7(11), 1437, 11935, 11719
[115, 5]	98	116, 137(10)5, 113, 15(11)(10)6, 13(11)(12)(10), 11(11)95, 119(12)(10), 15694, 15156, 126(12)9, 1(10)98, 119(12)5, 1275(10), 1588, 11917, 1229, 12(10)(12)4, 1118(10), 11(11)(12), 114(11)(10), 118(12)5, 1427(10), 1515(11)
[120, 5]	102	118(11), 169, 1127, 1, 124(12)3, 10(11), 11, 1338, 19(12)1(12), 13258, 1863, 128(10)4, 1274, 1161(10), 13438, 116(10)(12), 18(12)(11), 131(10)(11), 11814, 11363, 117(10)6, 12(10)28, 11(12)93, 13862

Table 4
Best QC codes over $\mathbb{F}_{13}$ with $p = 6$.

Code	d	$r_i(x)$
[12, 6]	7	12212, 11(10)93
[18, 6]	11	12, 10(12)5(11), 128(10)3
[24, 6]	16	185, 1827(12)4, 12835, 114947
[30, 6]	21	13, 11183(10), 1133(12)4, 14(10)2(11)(12), 13537
[36, 6]	26	1002, 118217, 115184, 126596, 12179, 1112
[42, 6]	32	11(10), 12(12)235, 111893, 1121(12)(12), 138745, 119(12)24, 13(12)6(11)(10)
[48, 6]	37	114, 107, 1(11)267, 1131(12), 128(11)(10)(11), 1346(11)5, 11(11)6(11)4, 1(12)511
[54, 6]	42	105(11)7, 118633, 19, 111299, 1698(10)3, 1269(11)8, 121976, 1451(11)4, 11(12)9(10)(11)
[60, 6]	47	1(11)(12), 104(10), 12(12)4(10)4, 1469(10), 119(10)6, 1(10)25(11), 11(11)38(11), 14(10)46, 15564, 12361
[66, 6]	52	13, 11, 1214, 10633, 1124(10)7, 141(11)8(10), 14187(11), 1455(11), 11(12)7(11)(12), 135843, 15577
[72, 6]	57	1, 11(11)5, 12(10)(10)(11), 11(11)543, 147(12)92, 1299, 128958, 111(12)(11)2, 15768, 11(12)61(10), 19247, 12773
[78, 6]	63	12(12)1, 19, 153(10)3(11), 13784(10), 19(10)3, 10326, 12(12)(10)85, 125268, 11(11)65, 13564, 187(11)9, 1192(10)7, 1(10)269
[84, 6]	68	119, 149, 18332, 13(10)17(12), 14623, 131768, 105(10)3, 11837(10), 11123(11), 121435, 1241(10)8, 151(10)7, 11385, 11(10)535
[90, 6]	73	106, 11, 11(11)68(11), 11398(11), 14(11)4(10), 143(11)2, 119(11)29, 125286, 10169, 17556, 13469(11), 129474, 1535, 108(10)(10), 13(11)2(10)5
[96, 6]	78	132345, 14535(12), 14(10)(12)82, 11(10)395, 1029, 112453, 115(10)68, 19452, 1231(12), 132(11)(12), 11286, 1(12)(12)(12)(12), 116684, 13(11)476, 147(12)(12), 1591
[102, 6]	83	102, 1432, 116735, 1263, 12(10)8, 1, 11123(12), 11585(12), 14689(11), 19432, 17(10)96, 124592, 117758, 1347(11), 1419(12)4, 12(11)7(12)(11), 14(12)(12)6
[108, 6]	88	1, 107, 149(11)1(12), 14(10)8(10)2, 121796, 11(12)173, 10249, 14142(12), 13(12)8(10)(11), 116, 116895, 126714, 11323(11), 1114(10)6, 1(11)684, 1901, 19(12)84, 13673
[114, 6]	94	104(11)7, 118(11)(10)8, 11(10)418, 1688(12), 15, 1(10)8(10)8, 125894, 112452, 1282(12)(10), 1(10)4(11)(10), 1178(10)2, 121752, 16(12)59, 14618, 135(12)15, 19(11)(10)2, 117(10)15, 113564, 16235(11)
[120, 6]	99	125, 119(11)56, 1432(12)6, 1, 16726, 101(12), 1382(11)(10), 19133, 107(11), 112(11)(11), 1427(10)6, 116459, 121(11)6, 1187(12)(10), 131645, 1(10)46, 146(10)(12)5, 112(10)(12)2, 1421(11)(10), 14(10)(11)9
[126, 6]	105	16, 11, 117(12)6, 125(12), 11668(12), 14(11)(10)92, 11(11)(12)18, 13(11)8(11)5, 10759, 114578, 111934, 11493(12), 1(10)91, 123575, 132193, 114188, 13(12)5(12)4, 119427, 1154(10)3, 14147(12), 12(11)3(12)4
[132, 6]	110	13, 17(10)72, 11, 19(12), 14295, 121(12)63, 119615, 11572(10), 116784, 14(11)1(10)2, 1(12)(10)(12)(11), 129234, 111114, 11598(11), 14935(11), 132398, 1(12)918, 1417(11)2, 141(11)53, 10927, 115(11)5(12), 1(10)(12)14
[138, 6]	115	112146, 12, 1(10)83, 119125, 17, 116(10)35, 1397, 11(11)683, 11(11)843, 145(11)68, 13026, 1(10)4(11)8, 10743, 1846(11), 1251(12)9, 11635, 112(11)(12)5, 129373, 164(12)2, 15(12)56, 14(11)818, 1328(11)4, 11032
[144, 6]	120	101, 1574(11), 121642, 19(11)28, 127(12)6(10), 139(10)62, 1(12)969, 16(11)2(11), 14(10)5(12), 125438, 1419(10)6, 119324, 12(12)45(11), 16(12), 13(12)3(12)2, 142(10)84, 1326(11)4, 15(11)(12)38, 1419, 129585, 13(11)434, 114897, 114(10)64, 12(11)6(10)

with weight distribution

i	A_i
0	1
15	9300
16	11640
17	51960
18	98520
19	125220
20	74652

This code is also optimal since it meets the Griesmer bound (1), and so establishes that $d_{13}(20, 5) = 15$. In addition, the codes for $m = 3$ and 4 with $p = 5$ meet the Griesmer bound. Note that all codes with $n \leqslant 14$ given in the tables are MDS.

References

[1] K. Betsumiya, S. Georgiou, T.A. Gulliver, M. Harada, C. Koukouvinos, On self-dual codes over some prime fields, Discrete Math. 262 (2003) 37–58.
[2] W. Bosma, J. Cannon, Handbook of Magma Functions, Department of Mathematics, University of Sydney, available online at http://magma.maths.usyd.edu.au/magma/.
[3] R.N. Daskalov, T.A. Gulliver, New good quasi-cyclic ternary and quaternary linear codes, IEEE Trans. Inform. Theory 43 (1997) 1647–1650.
[4] M.A. de Boer, Almost MDS codes, Des. Codes Cryptogr. 9 (1996) 143–155.
[5] J.A. Gallian, Contemporary Abstract Algebra, 4th ed., Narosa Publishing House, New Delhi, 1999.
[6] F. Glover, Tabu search—Part I, ORSA J. Comput. 1 (1989) 190–206.
[7] M. Grassl, Bounds on the minimum distance of linear codes and quantum codes, available online at http://www.codetables.de.
[8] P.P. Greenough, R. Hill, Optimal ternary quasi-cyclic codes, Des. Codes Cryptogr. 2 (1992) 81–91.
[9] T.A. Gulliver, New optimal ternary linear codes, IEEE Trans. Inform. Theory 41 (1995) 1182–1185.
[10] T.A. Gulliver, V.K. Bhargava, Some best rate $1/p$ and rate $(p-1)/p$ systematic quasi-cyclic codes over GF(3) and GF(4), IEEE Trans. Inform. Theory 38 (1992) 1369–1374.
[11] T.A. Gulliver, V.K. Bhargava, New good rate $(m-1)/pm$ ternary and quaternary quasi-cyclic codes, Des. Codes Cryptogr. 7 (1996) 223–233.
[12] I.S. Honkala, P.R.J. Östergård, Applications in code design, in: E.H.L. Aarts, J.K. Lenstra (Eds.), Local Search in Combinatorial Optimization, Wiley, New York, 2003.
[13] F.J. MacWilliams, N.J.A. Sloane, The Theory of Error-Correcting Codes, North-Holland, New York, 1977.
[14] D.W. Newhart, On minimum weight codewords in QR codes, J. Combin. Theory Ser. A 48 (1988) 104–119.
[15] G. Royle, Polya counting I, available online at http://undergraduate.csse.uwa.edu.au/units/CITS7209/polya.pdf.
[16] J. van Lint, R. Wilson, A Course Combinatorics, Cambridge University Press, Cambridge, 1992.